TO: USPTO

ZILKA·KOTAB PC

ZILKA, KOTAB & FEECE™

95 SOUTH MARKET ST., SUITE 420
SAN JOSE, CA 95113

TELEPHONE (408) 971-2573
FAX (408) 971-4660

FAX COVER SHEET

Date: October 13, 2005	Phone Number	Fax Number
To: Board of Patent Appeals		(571) 273-8300
From: Kevin J. Zilka		

Docket No.: NAIIP344_01.249.01 **App. No: 10/028,412**

Total Number of Pages Being Transmitted, Including Cover Sheet: 35

Message:

Please deliver to the Board of Patent Appeals.

Thank you,

Kevin J. Zilka

☐ *Original to follow Via Regular Mail* X *Original will Not be Sent* ☐ *Original will follow Via Overnight Courier*

IF YOU DO NOT RECEIVE ALL PAGES OR IF YOU ENCOUNTER
ANY OTHER DIFFICULTY, PLEASE PHONE Erica
AT (408) 971-2573 AT YOUR EARLIEST CONVENIENCE

Practitioner's Docket No. NAI1P344/01.249.01 ***PATENT***

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Alex J. Hinchliffe et al.

Application No.: 10/028,412 Group No.: 2143
Filed: 12/21/2001 Examiner: Dennison, Jerry
For: DESKTOP SECURITY IN PEER-TO-PEER NETWORKS

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. Transmitted herewith, in triplicate, is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on September 13, 2005.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*
(When using Express Mail, the Express Mail label number is mandatory; Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

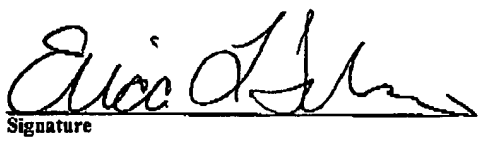
_ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)
_ with sufficient postage as first class mail.

37 C.F.R. § 1.10*
_ as "Express Mail Post Office to Addressee"
Mailing Label No. _____ (mandatory)

TRANSMISSION
✓ facsimile transmitted to the Patent and Trademark Office, (571) 273-87300.

Date: 10/13/05



Signature

Erica L. Farlow

(type or print name of person certifying)

** Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	$500.00
Appeal Brief fee due	**$500.00**

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$500.00
Extension fee (if any)	$0.00
TOTAL FEE DUE	**$500.00**

6. FEE PAYMENT

Authorization is hereby made to charge the amount of $500.00 to Deposit Account No. 50-1351 (Order No. NAI1P344).

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P344).

Signature of Practitioner
Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

RECEIVED
CENTRAL FAX CENTER

OCT 13 2005

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	
Hinchliffe et al.	Art Unit: 2143
Application No. 10/028,412	Examiner: Dennison, Jerry B.
Filed: December 21, 2001	Date: October 13, 2005
For: DESKTOP SECURITY IN PEER-TO-PEER NETWORKS	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on September 13, 2005.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS
V SUMMARY OF CLAIMED SUBJECT MATTER
VI GROUNDS OF REJECTION PRESENTED FOR REVIEW

10/14/2005 HDEMESS1 00000012 501351 10028412
01 FC:1402 500.00 DA

VII ARGUMENTS

VIII APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY THE APPELLANT IN THE APPEAL

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

Since no such proceedings exist, no Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1, 2, 4, 5, 7, 9-16, 18, 19, 21, 23-30, 32, 33, 35, and 37 - 49

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1, 2, 4, 5, 7, 9-16, 18, 19, 21, 23-30, 32, 33, 35, and 37 - 49
3. Claims allowed: None
4. Claims rejected: 1, 2, 4, 5, 7, 9-16, 18, 19, 21, 23-30, 32, 33, 35, and 37 - 49

C. CLAIMS ON APPEAL

The claims on appeal are: 1, 2, 4, 5, 7, 9-16, 18, 19, 21, 23-30, 32, 33, 35, and 37 - 49

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, an amendment was filed August 3, 2005. In the Advisory Action dated August 25, 2005, the Examiner did not enter such amendment because new issues were raised which would require further search and consideration.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claim 1 et al., as shown in Figure 2, a computerized method is provided which monitors a peer-to-peer network for suspicious activity based on patterns of activity (e.g. item 200 of Figure 2). An action associated with a particular pattern is performed when the particular pattern is detected in the peer-to-peer network (e.g. item 207 of Figure 2). Also, the peer-to-peer network permits peers to connect and operate substantially without a server by utilizing the server, at most, for providing addresses for the peers in the peer-to-peer network. Furthermore, a pattern of activity is defined in terms of a configuration of shared data on a peer, where the configuration establishes a baseline of authorized shares and permissions in association with the shared data. In use, the monitoring of the peer-to-peer network comprises evaluating a change with respect to the shared data on a peer in the peer-to-peer network, where the change is made with respect to the baseline. Note paragraph [0021] on page 9 – paragraph [0023] on page 10, for example.

VI GROUNDS OF REJECTION PRESENTED FOR REVIEW
(37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue #1: The Examiner has rejected Claims 1, 15, 29, 45 and 48 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which appellant regards as the invention.

Issue #2: The Examiner has rejected Claims 1, 2, 5, 11, 15, 16, 19, 25, 30, 33, 39 and 45-49 under 35 U.S.C. 103(a) as being unpatentable over Welch, Jr. et al., U.S. Patent No. 5,862,335, in view of Meadway et al., U.S. Patent No. 6,675,205.

Issue #3: The Examiner has rejected Claims 4, 7, 9, 10, 12-14, 18, 21, 23, 24, 26-28, 32, 35, 37, 38 and 40-44 under 35 U.S.C. 103(a) as being unpatentable over Welch, Jr. et al., U.S. Patent No. 5,862,335, in view of Meadway et al., U.S. Patent No. 6,675,205, in further view of Conklin et al., U.S. Patent No. 5,991,881.

VII ARGUMENTS (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue #1:

The Examiner has rejected Claims 1, 15, 29, 45 and 48 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which appellant regards as the invention.

Group #1: Claims 1, 15 and 29

The Examiner has stated that it is unclear to the Examiner what "and operate substantially" means. The Examiner has also stated that it is unclear as to what is required by the server and that using the server for anything is an option. However, appellant respectfully asserts that the claim language in the foregoing claims expressly states that "the peer-to-peer network permits peers to connect and operate substantially without a server by utilizing the server, at most, for providing addresses for the peers in the peer-to-peer network" (emphasis added). Thus, the peers, at most, use the server for providing addresses for the peers in the peer-to-peer network.

Group #2: Claim 45

The Examiner has stated that it is unclear what the claim language means, what is taking action and what action is taken. Appellant respectfully asserts the "share configuration loop is executed to...take action as a function of a type of the changes" (emphasis added). Appellant further asserts that the actual action taken is not claimed and would unduly limit such claim.

Group #3: Claim 48

The Examiner has stated that it is unclear why the configuration loop examines against a previously recorded share configuration. Appellant respectfully asserts that claiming a reason why "the share configuration loop examines a current share configuration against a previously recorded shared configuration" would unduly limit such claim by limiting the function to a claimed purpose.

Issue #2:

The Examiner has rejected Claims 1, 2, 5, 11, 15, 16, 19, 25, 29, 30, 33, 39 and 45-49 under 35 U.S.C. 103(a) as being unpatentable over Welch, Jr. et al., U.S. Patent No. 5,862,335, in view of Meadway et al., U.S. Patent No. 6,675,205.

Group #1: Claims 1, 2, 15, 16, 29 and 30

It is noted that the Examiner has attempted to interpret appellant's claimed peer-to-peer network to refer to, for example, any client and server communications. Appellant respectfully disagrees with this interpretation, especially in view of the previous amendments which require that "the peer-to-peer network permits peers to connect and operate substantially without a server by utilizing the server, at most, for providing addresses for the peers in the peer-to-peer network."

The Examiner has relied on the following excerpts from Meadway to make a prior art showing of appellant's claimed "performing an action associated with a particular pattern when the particular pattern is detected in the peer-to-peer network" (see this or similar, but not identical language in each of the foregoing claims).

> "Expanding on the above concepts, the invented system is a service which performs centralized searches based on index information transmitted by peer systems to the central site using an agent program running on each peer, and then directs the peer systems to each other for the purpose of retrieving files." (Col. 1, lines 45-52-emphasis added)

> "...the file is sent by the system containing the file either to the central site or directly to the user who requested the file via email attachment." (Col. 1, lines 63-65)

> "agent program downloaded and installed by each peer system user. This agent program is described in detail in pending U.S. patent application Ser. Nos. 09/419,405, U.S. Pat. No. 6,516,337, and 09/575,971, filed May 23, 2000, by the same inventors which are hereby incorporated by reference. The indexing process on each system may be initiated manually or on a scheduled basis, with updates transmitted whenever the user connects to the central service." (Col. 2, lines 1-10)

Appellant respectfully asserts that the excerpts relied on by the Examiner simply relate to "direct[ing] the peer systems to each other for the purpose of retrieving files" (see emphasized excerpt above). In no way do such excerpts teach appellant's specific claim language, namely "performing an action associated with a particular pattern when the particular pattern is detected..." (emphasis added), especially when read in the context of the remaining claim language where "suspicious activity [is monitored] based on [the] patterns of activity" (emphasis added). Clearly, only generally directing peer systems to each other, as in Meadway, does not meet "performing an action associated with a particular pattern" where such monitoring is with respect to "suspicious activity," in the context claimed by appellant.

The Examiner has also relied on the above cited excerpts to make a prior art showing of appellant's claimed technique "wherein a pattern of activity is defined in terms of a configuration of shared data on a peer, the configuration establishing a baseline of authorized shares and permissions in association with the shared data." Appellant respectfully asserts that that nowhere in the above excerpts is there even any mention of defining the pattern of activity "in terms of a configuration of shared data on a peer, the configuration establishing a baseline of authorized shares and permissions in association with the shared data," as claimed by appellant (emphasis added).

Instead, Meadway simply teaches that "index information [is] transmitted by peer systems to the central site using an agent program running on each peer, and then...the peer systems [are directed] to each other for the purpose of retrieving files" (see excerpts above). Appellant notes that such indexed information relates to the "contents of the files" (see Col. 2, line15), and therefore, no baseline of

authorized shares and permissions is established in Meadway, in the context claimed by appellant.

The Examiner has again relied on the above cited excerpts to make a prior art showing of appellant's claimed technique "wherein monitoring a peer-to-peer network comprises evaluating a change with respect to the shared data on a peer in the peer-to-peer network, the change being made with respect to the baseline." Appellant asserts that such excerpts yet again fail to teach "evaluating a change with respect to the shared data on a peer in the peer-to-peer network, the change being made with respect to the baseline," as claimed by appellant (emphasis added). In the excerpts above, Meadway discloses that "updates [are] transmitted whenever the user connects to the central service." However, such updates relate to the indexing process, as disclosed in the excerpts above, and not "evaluating a change...with respect to the baseline" where such baseline is of "authorized shares and permissions in association with the shared data," as claimed by appellant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Thus, a notice of allowance or a specific prior art showing of all of appellant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Group #2: Claims 5, 19 and 33

The Examiner has relied on Col. 3, lines 25-30 and 45-50 in Welch to make a prior art showing of appellant's claimed "pattern of activity [that] is defined in terms of network traffic in the peer-to-peer network that uses a specific protocol." Appellant notes, however, that such excerpts from Welch only generally disclose "analyz[ing] logical connections and file transfers...by examining the information of layers 2,3, and 4" where "protocol control information 42 [is] available in layers 2, 3, 4 and 7 of a packet." Only generally examining protocol control information, however, does not meet appellant's claimed "pattern of activity", let alone "a pattern of activity [that] is defined in terms of network traffic...that uses a specific protocol" (emphasis added).

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #3: Claims 11, 25 and 39

The Examiner has relied on the following excerpt from Welch to make a prior art showing of appellant's claimed technique "wherein the patterns of activity are local to a peer in the peer-to-peer network."

> "...a copy of the revised connection record 93 to the archive. This allows dynamic display of connection activity. Analysis of the packet complete, CME 83 branches to step 204.
>
> Thus, methods of monitoring both local connections and file transfers in a computer network have been described." (Col. 10, lines 5-10)

Appellant respectfully asserts that such excerpt merely discloses "monitoring...local connections and file transfers." Clearly, mere local connections do not meet appellant's claimed "patterns of activity [that] are local to a peer in the peer-to-peer network" (emphasis added).

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #4: Claim 45

The Examiner has relied on the following excerpt from Meadway to make a prior art showing of appellant's claimed "wherein a share configuration loop is executed to detect changes to shares and corresponding permissions, and take an action as a function of a type of the changes."

> "...agent program downloaded and installed by each peer system user. This agent program is described in detail in pending U.S. patent application Ser. Nos. 09/419,405, U.S. Pat. No. 6,516,337, and 09/575,971, filed May 23, 2000, by the same inventors which are hereby incorporated by reference. The indexing process on each system may be initiated manually or on a scheduled basis, with updates transmitted whenever the user connects to the central service.
>
> The agent is also responsible for transmitting copies of the requested file to the systems whose requests are waiting..." (Col. 2, lines 1-10)

Appellant respectfully asserts that the agent program disclosed in Meadway is simply associated with the indexing process where the index is of "the contents of the files" on peers (see Col. 2, lines 14-15). Simply nowhere in Meadway is there even any mention of a "share configuration loop [that] is executed to detect changes to shares and corresponding permissions, and take an action as a function of a type of the change," as claimed by appellant (emphasis added).

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #5: Claim 46

The Examiner has again relied on Col. 2, lines 1-10 of Meadway to make a prior art showing of appellant's claimed technique "wherein the share configuration loop is executed dynamically." Appellant respectfully asserts that such excerpt along with the entire Meadway reference fail to meet appellant's claimed "share configuration loop," and thus also cannot meet the instant claim language further describing the claimed share configuration loop. Again, appellant respectfully asserts that the agent program disclosed in Meadway is merely associated with the indexing process where the index is of "the contents of the files" on peers (see Col. 2, lines 14-15). Simply nowhere in Meadway is there even any mention of a "share configuration loop [that] is executed dynamically," as claimed by appellant (emphasis added).

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #6: Claim 47

The Examiner has again relied on Col. 2, lines 1-10 of Meadway to make a prior art showing of appellant's claimed technique "wherein the share configuration loop is executed on a schedule." Appellant respectfully asserts that such excerpt along with the entire Meadway reference fail to meet appellant's claimed "share configuration loop" and thus also cannot meet the instant claim language further describing the claimed share configuration loop. Again, appellant respectfully asserts that the agent program disclosed in Meadway is merely associated with the indexing process where the index is of "the contents of the files" on peers (see Col. 2, lines 14-15). Simply nowhere in Meadway is there even any mention of a "share configuration loop [that] is executed on a schedule," as claimed by appellant (emphasis added).

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #7: Claim 48

The Examiner has again relied on Col. 2, lines 1-10 of Meadway to make a prior art showing of appellant's claimed technique "wherein the share configuration loop examines a current share configuration against a previously recorded shared configuration." Appellant respectfully asserts that such excerpt along with the entire Meadway reference fail to meet appellant's claimed "share configuration loop" and thus also cannot meet the instant claim language further describing the claimed share configuration loop. Again, appellant respectfully asserts that the agent program disclosed in Meadway is merely associated with the indexing process where the index is of "the contents of the files" on peers (see Col. 2, lines 14-15). Simply nowhere in Meadway is there even any mention of a "share configuration loop [that] examines a current share configuration against a previously recorded shared configuration," as claimed by appellant (emphasis added).

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #8: Claim 49

The Examiner has yet again relied on Col. 2, lines 1-10 along with Col. 2 lines 35-41 in Meadway to make a prior art showing of appellant's claimed technique where "if the change includes an attempt to un-share a file or directory, the action includes a log entry." Appellant asserts that such excerpts do not teach any sort of "attempt to un-share a file or directory" as claimed by appellant, but instead only disclose indexing the contents of files and an "agent that reports to the central server the identities of files on the computer that will be provided if requested by others." In addition, such excerpts also fail to teach "a log entry" action if a change is made with respect to un-sharing a file or directory, in the manner claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Issue #3:

The Examiner has rejected Claims 4, 7, 9, 10, 12-14, 18, 21, 23, 24, 26-28, 32, 35, 37, 38 and 40-44 under 35 U.S.C. 103(a) as being unpatentable over Welch, Jr. et al., U.S. Patent No. 5,862,335, in view of Meadway et al., U.S. Patent No. 6,675,205, in further view of Conklin et al., U.S. Patent No. 5,991,881.

Group #1: Claims 4, 10, 12, 18, 24, 26, 32, 38 and 40-42

Appellant respectfully asserts that such claims are not met by the prior art for the reasons argued with respect to Issue #1, Group #1.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #2: Claims 7, 21 and 35

The Examiner has relied on the following excerpt from Conklin to make a prior art showing of appellant's claimed "pattern of activity [that] is defined in terms of network traffic in the peer-to-peer network having a foreign address."

> "When a packet or accumulation of packets match a predefined intrusion profile the Intrusion Detection function identifies the network traffic as a reportable activity will construct a data structure which contains a date/time stamp indicating the time of detection, the source and destination Internet Protocol (IP) addresses, an assigned message identifying the event detected. This data structure is passed to the Alert Notification function for processing. When a positive identification of a reportable activity occurs, the entire triggering packet(s) may be written to a log file created in the Evidence Logging function." (Col. 5, lines 25-35-emphasis added)

Appellant respectfully asserts that the above excerpt from Conklin only teaches that "[when] a packet or accumulation of packets match a predefined intrusion profile

[then] a data structure [will be constructed] which contains...the source and destination...addresses" (see emphasized excerpt above). Thus, the pattern of activity in Conklin is not taught to be "defined in terms of network traffic...having a foreign address," as claimed by appellant, but instead only general source and destination addresses are reported after the match is made.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #3: Claims 9, 23 and 37

The Examiner has relied on Col. 5, lines 33-35 of Conklin, as excerpted above, to make a prior art showing of appellant's claimed technique "wherein the action comprises logging information about the particular pattern." However, appellant respectfully asserts that only "the entire triggering packet(s) [are] written to a log file" in Conklin (emphasis added), and not "information about the particular pattern," as claimed by appellant (emphasis added).

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #4: Claims 13, 27 and 43

The Examiner has relied on Col. 4, lines 45-55 in Conklin to make a prior art showing of appellant's claimed "obtaining a set of rules specifying the patterns of activity and associated actions." Appellant notes, however, that the above excerpt in Conklin completely fails to even mention "a set of rules specifying the patterns of activity and associated actions," as claimed by appellant (emphasis added). In fact, even the Examiner, in his rejection, states that "Conklin disclosed obtaining pre-stored patterns of activity in a database," but fails to address any "associated actions" as in appellant's claim language.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #5: Claims 14, 28 and 44

The Examiner has relied on the following excerpt from Conklin to make a prior art showing of appellant's claimed "refreshing the set of rules when the set of rules changes."

> "the Intrusion Detection function examines the data in comparison to a series of predefined or learned patterns which are pre-stored or developed from data received from the network.
>
> In the preferred embodiment, the network data is compared to a database of known patterns." (Col. 4, lines 48-52)

Appellant respectfully asserts that the above excerpt merely discloses comparing "the data...to a series of predefined or learned patterns which are pre-stored." However, nowhere in such excerpt or the entire Conklin reference is there any suggestion of "refreshing the set of rules when the set of rules changes," as claimed by appellant (emphasis added).

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII APPENDIX OF CLAIMS (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A computerized method comprising:

monitoring a peer-to-peer network for suspicious activity based on patterns of activity; and

performing an action associated with a particular pattern when the particular pattern is detected in the peer-to-peer network;

wherein the peer-to-peer network permits peers to connect and operate substantially without a server by utilizing the server, at most, for providing addresses for the peers in the peer-to-peer network;

wherein a pattern of activity is defined in terms of a configuration of shared data on a peer, the configuration establishing a baseline of authorized shares and permissions in association with the shared data;

wherein monitoring a peer-to-peer network comprises evaluating a change with respect to the shared data on a peer in the peer-to-peer network, the change being made with respect to the baseline.

2. (Original) The computerized method of claim 1, wherein monitoring a peer-to-peer network comprises:

evaluating network traffic among peers in the peer-to-peer network.

3. (Cancelled)

4. (Original) The computerized method of claim 1, wherein a pattern of activity is defined in terms of a threshold value of network traffic in the peer-to-peer network.

5. (Original) The computerized method of claim 1, wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network that uses a specific protocol.

6. (Cancelled)

7. (Original) The computerized method of claim 1, wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network having a foreign address.

8. (Cancelled)

9. (Original) The computerized method of claim 1, wherein the action comprises logging information about the particular pattern.

10. (Original) The computerized method of claim 1, wherein the action comprises sending an alert about the particular pattern.

11. (Original) The computerized method of claim 1, wherein the patterns of activity are local to a peer in the peer-to-peer network.

12. (Original) The computerized method of claim 1, wherein the patterns of activity are global to the peer-to-peer network.

13. (Original) The computerized method of claim 1 further comprising:

obtaining a set of rules specifying the patterns of activity and associated actions.

14. (Original) The computerized method of claim 13 further comprising:

refreshing the set of rules when the set of rules changes.

15. (Previously Presented) A computer-readable medium having executable instructions to cause a processor to perform a method comprising:

monitoring a peer-to-peer network for suspicious activity based on patterns of activity; and

performing an action associated with a particular pattern when the particular pattern is detected in the peer-to-peer network;

wherein the peer-to-peer network permits peers to connect and operate substantially without a server by utilizing the server, at most, for providing addresses for the peers in the peer-to-peer network;

wherein a pattern of activity is defined in terms of a configuration of shared data on a peer, the configuration establishing a baseline of authorized shares and permissions in association with the shared data;

wherein monitoring a peer-to-peer network comprises evaluating a change with respect to the shared data on a peer in the peer-to-peer network, the change being made with respect to the baseline.

16. (Original) The computer-readable medium of claim 15, wherein the method further comprises:

evaluating network traffic among peers in the peer-to-peer network when monitoring the peer-to-peer network.

17. (Cancelled)

18. (Original) The computer-readable medium of claim 15, wherein a pattern of activity is defined in terms of a threshold value of network traffic in the peer-to-peer network.

19. (Original) The computer-readable medium of claim 15, wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network that uses a specific protocol.

20. (Cancelled)

21. (Original) The computer-readable medium of claim 15, wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network having a foreign address.

22. (Cancelled)

23. (Original) The computer-readable medium of claim 15, wherein the action comprises logging information about the particular pattern.

24. (Original) The computer-readable medium of claim 15, wherein the action comprises sending an alert about the particular pattern.

25. (Original) The computer-readable medium of claim 15, wherein the patterns of activity are local to a peer in the peer-to-peer network.

26. (Original) The computer-readable medium of claim 15, wherein the patterns of activity are global to the peer-to-peer network.

27. (Original) The computer-readable medium of claim 15, wherein the method further comprises:

obtaining a set of rules specifying the patterns of activity and associated actions.

28. (Original) The computer-readable medium of claim 27, wherein the method further comprises:

refreshing the set of rules when the set of rules changes.

29. (Previously Presented) A system comprising:

a processor coupled to a memory through a bus;

a network interface coupled to the processor through the bus and further operable to selectively couple to a peer-to-peer network; and

a peer-to-peer security process executed by the processor from the memory to cause the processor to monitor the peer-to-peer network for suspicious activity based on patterns of activity, and to perform an action associated with a particular pattern when the particular pattern is detected in the peer-to-peer network;

wherein the peer-to-peer network permits peers to connect and operate substantially without a server by utilizing the server, at most, for providing addresses for the peers in the peer-to-peer network;

wherein a pattern of activity is defined in terms of a configuration of shared data on a peer, the configuration establishing a baseline of authorized shares and permissions in association with the shared data;

wherein monitoring a peer-to-peer network comprises evaluating a change with respect to the shared data on a peer in the peer-to-peer network, the change being made with respect to the baseline.

30. (Original) The system of claim 29, wherein peer-to-peer security process further causes the processor to evaluate network traffic between the peers in the peer-to-peer network when monitoring the peer-to-peer network.

31. (Cancelled)

32. (Original) The system of claim 29, wherein the peer-to-peer security process further causes the processor to monitor the peer-to-peer network for a pattern of

activity defined in terms of a threshold value of network traffic in the peer-to-peer network.

33. (Original) The system of claim 29, wherein the peer-to-peer security process further causes the processor to monitor the peer-to-peer network for a pattern of activity defined in terms of network traffic in the peer-to-peer network that uses a specific protocol.

34. (Cancelled)

35. (Original) The system of claim 29, wherein the peer-to-peer security process further causes the processor to monitor the peer-to-peer network for a pattern of activity defined in terms of network traffic having a foreign address.

36. (Cancelled)

37. (Original) The system of claim 29, wherein the peer-to-peer security process further causes the processor to log information about the particular pattern when performing the action associated with the particular pattern.

38. (Original) The system of claim 29, wherein the peer-to-peer security process further causes the processor to send an alert about the particular pattern when performing the action associated with the particular pattern.

39. (Original) The system of claim 29, wherein the system is a peer in the peer-to-peer network and the patterns of activity are local to the system.

40. (Original) The system of claim 29, wherein the system is a server in the peer-to-peer network and the patterns of activity are global to the peer-to-peer network.

41. (Original) The system of claim 40, wherein the system is a border firewall.

42. (Original) The system of claim 40, wherein the system is a domain name server.

43. (Original) The system of claim 29, wherein the peer-to-peer security process further causes the processor to obtain a set of rules specifying the patterns of activity and associated actions.

44. (Original) The system of claim 43, wherein the peer-to-peer security process further causes the processor to refresh the set of rules when the set of rules changes.

45. (Previously Presented) The computerized method of claim 1, wherein a share configuration loop is executed to detect changes to shares and corresponding permissions, and take action as a function of a type of the changes.

46. (Previously Presented) The computerized method of claim 45, wherein the share configuration loop is executed dynamically.

47. (Previously Presented) The computerized method of claim 45, wherein the share configuration loop is executed on a schedule.

48. (Previously Presented) The computerized method of claim 45, wherein the share configuration loop examines a current share configuration against a previously recorded shared configuration.

49. (Previously Presented) The computerized method of claim 45, wherein, if the change includes an attempt to un-share a file or directory, the action includes a log entry.

IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY THE APPELLANT IN THE APPEAL (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P344_01.249.01).

Respectfully submitted,

By: _____ Date: 10/13/05

Kevin J. Zilka

Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660